VENTURE FORAGERS

Future of Mobility – Automotive Cybersecurity

Our Team

Kateryna Kharenko is an MBA Candidate at the Wharton School with a focus on Business Analytics and a co-founder of MetalLight – metal-harvesting light for off-grid communities. Prior to Wharton, she worked at McKinsey & Company where she focused on strategy, due diligence and operations for industrial companies, and at KPMG corporate finance. Kateryna earned her BA and MA degrees in International Finance at the Taras Shevchenko National University of Kyiv.

Reynaldo Kirton is an MBA Candidate at the Wharton School with a focus on Finance and Entrepreneurship. Reynaldo is currently interning at Harlem Capital. Prior to Wharton, Reynaldo was a consultant at Altman Vilandrie & Co. where he performed due diligence on target companies in the TMT industry. Reynaldo earned his B.A. at Harvard where he majored in Economics and played football.

Ryan Kramer is an MBA Candidate at the Wharton School with a focus on Finance and Entrepreneurship. Prior to Wharton, he served as an Air Force Acquisitions Officer evaluating emerging space technologies and was a product manager in the Air Force's partnerships with both early-stage startups and large defense contractors. He also deployed overseas with USSOCOM leading the standup of contractor drone sites.

M. Savio Nicholas is an MBA Candidate at the Wharton School with a focus on Business Analytics and Strategic Management. Prior to Wharton, Savio co-founded Sift, a B2B startup that helps managers build better teams. Savio is a Michigan Engineering grad, a former VC intern at RPM Ventures, and a 2014 Venture for America Fellow.

Experts Consulted

Tamir Bechor, PhD

Co-founder of Cymotive

Chris Valasek

Autonomous Vehicle Security Architect at Cruise

Federicco Maggi

Senior Researcher at Trend Micro

Alexander Gounares

CEO of Polyverse

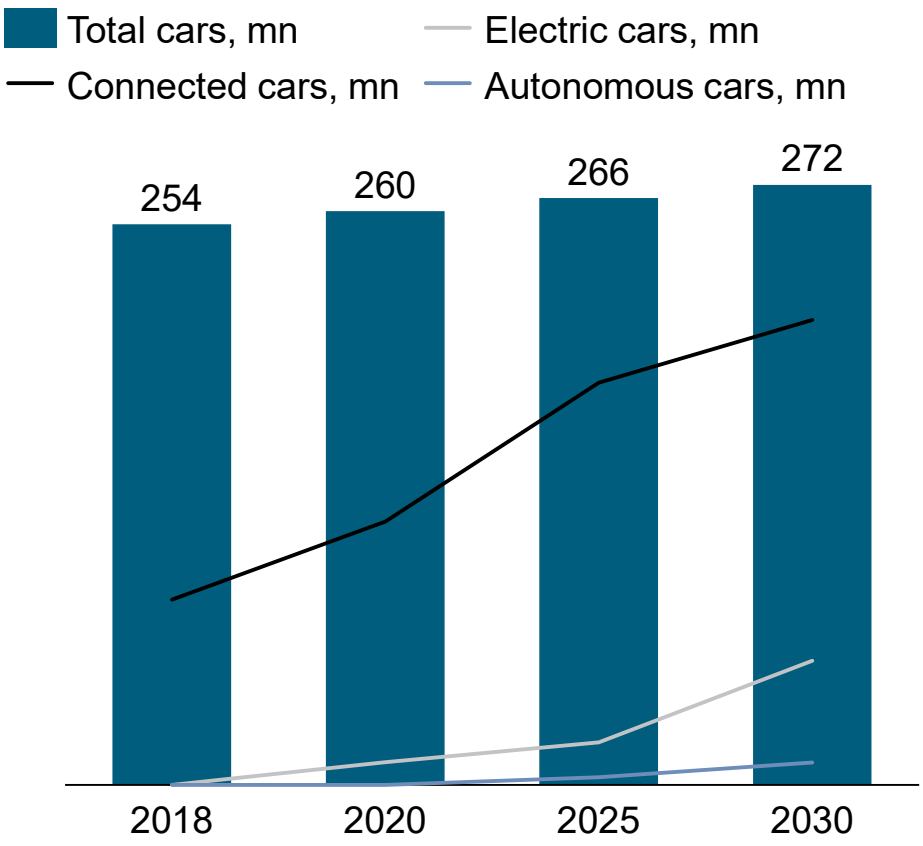
Scott Frank

VP Marketing at Airbiquity

Automotive Cybersecurity Market Size and Growth Drivers

Connected Vehicles Expected to Grow at ~8% CAGR through 2030

Connected cars penetration in the US is expected to grow up to ~80% by 2030…



Souce: Strategy&, Accenture

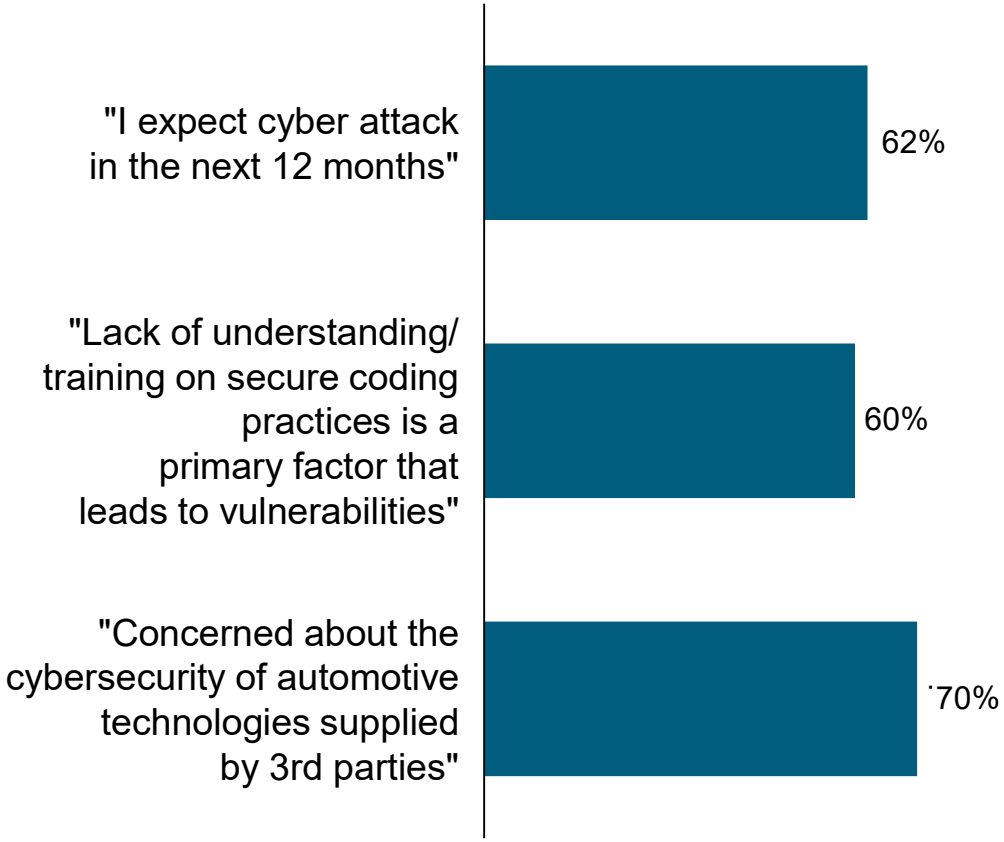
… driven by overall technology development & market demand

Key drivers of connected vehicle growth:

- **5G connectivity:** availability of infrastructure to vehicle communication, alternatives to GPS
- **Autonomy:** L4 is expected to be operating in selected cities by 2020-2025
- **Shared economy:** 48% of US consumers would consider giving up their own car if autonomous mobility solutions were available

Increasing Cybersecurity Concern Spurs Market Growth

Cybersecurity is increasingly becoming a concern among automakers…



Souce: Ponemon Institute survey, VDOO

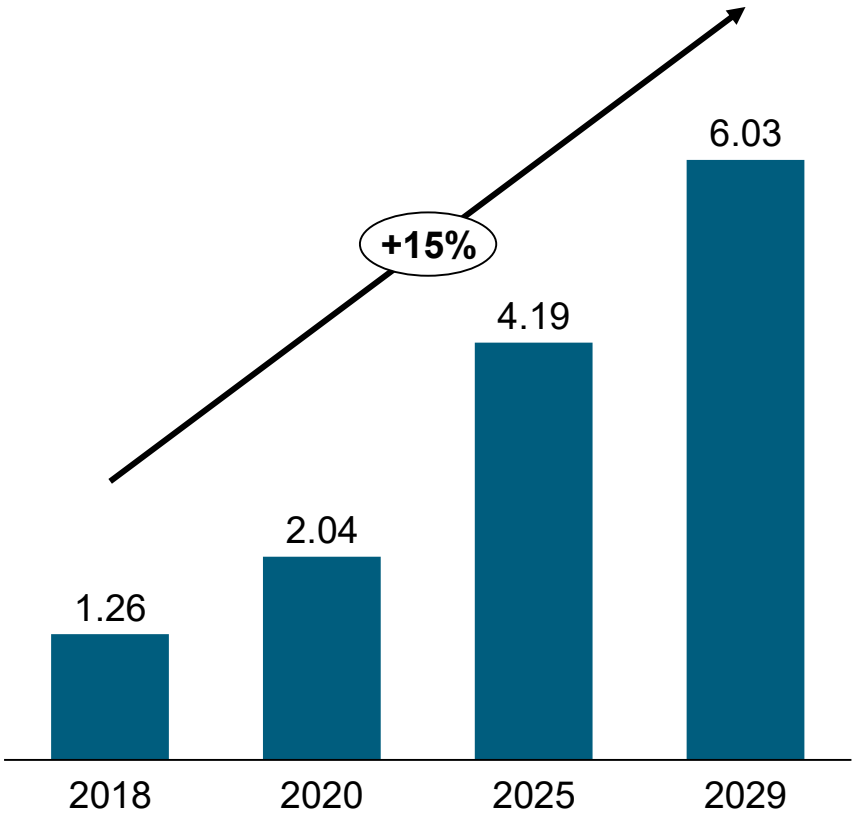
… which is also pressured by regulations

Regulation projects in place:

- **Global Auto Alliance:** Framework for Automotive Cybersecurity Best Practices
- **Society of Automotive Engineers:** SAE J3061, draft ISO/SAE 21434
- **US Congress:** SPY Car Act of 2019
- **UN:** ECE-TRANS-WP29-GRVA

Market Opportunity Reflected in Market Growth and Investment Activity

Global Automotive cybersecurity market is $1.5B, expected to grow ~ 15% p.a.



Many recent deals in the space come from automotive suppliers

ARGUS CYBER SECURITY	Acquired by Continental 2017
NDIAS	JV between Denso & NRI 2018
TRUSTPOINT	Acquired by ETAS (Bosch) 2017
Advanced Telematic SYSTEMS	Acquired by HERE 2018
TOWERSEC AUTOMOTIVE CYBER SECURITY	Acquired by Harman 2016
ARILOU	Acquired by NNG 2016
CanBusHack	Acquired by Trillium 2017
dellfer	Seed by Denso 2018

Souce: BIS research

Market is defined as sales of intrusion detection system (IDS) and intrusion detection and prevention system (IDPS)

Key Takeaways

The importance of automotive cyber security is growing

1 Connected vehicles are an established sector of the automotive industry

- ~80% of vehicles will be connected by 2030

2 Connected vehicles are being hacked more, and OEMs are aware of vulnerabilities

- Hacking is a large problem for OEMs
- Cyber risks pose significant reputational threat
- OEMs may soon be required by law to disclose cyber threats

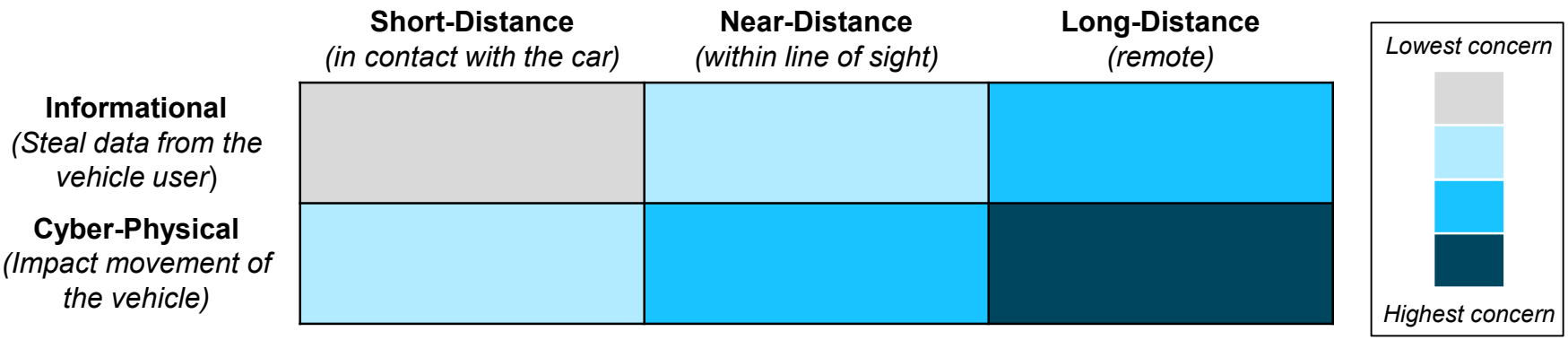
3 OEMs/suppliers don't have capabilities for cyber security and are willing to invest

- OEMs/suppliers traditionally focus on hardware and not software
- They are willing to invest in capabilities they can't develop in-house

Automotive Cybersecurity Attack Vectors

Automotive Cyber-attacks can be Categorized by Range and Intent

Remote cyber-physical attacks pose the greatest threat

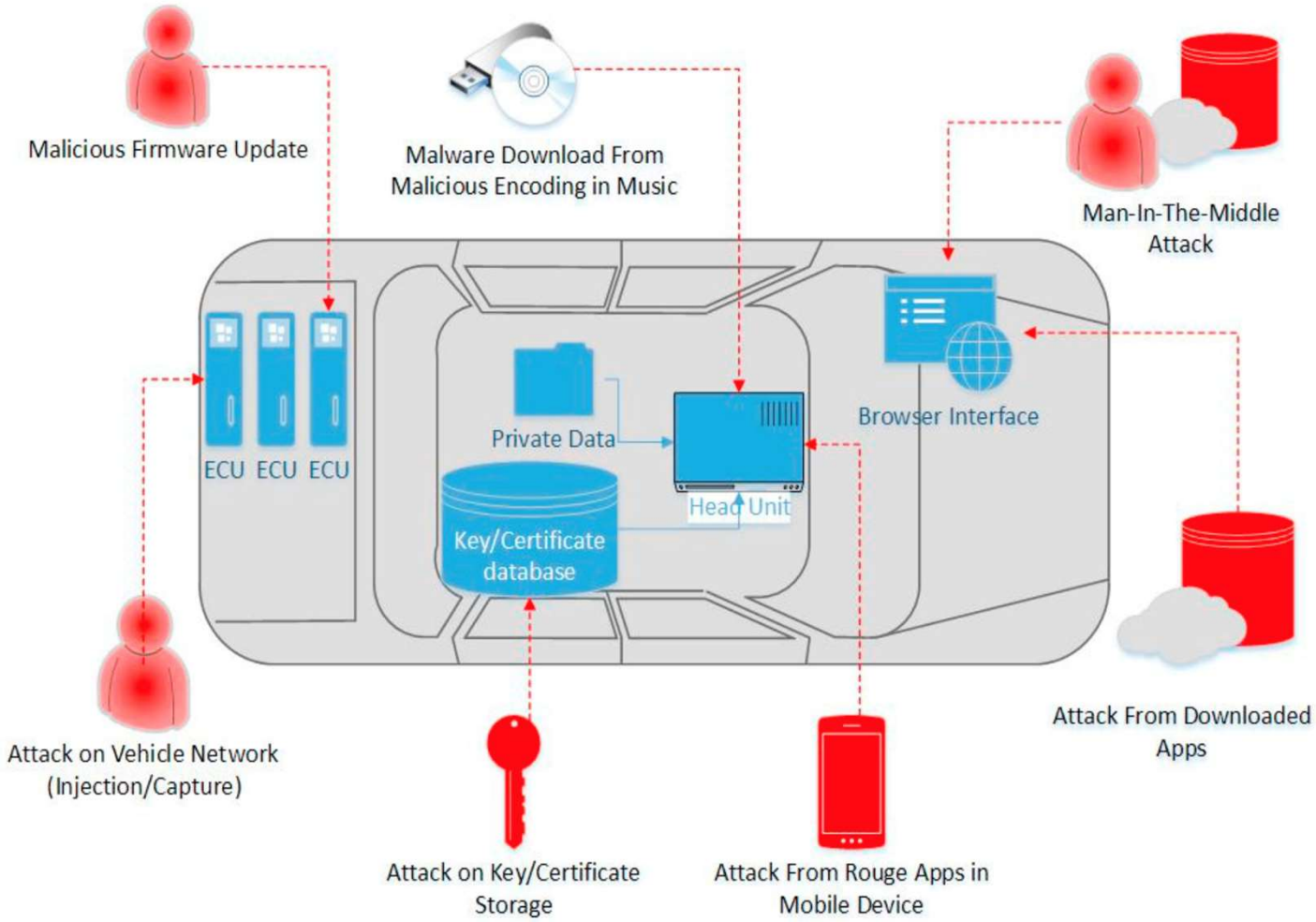


Known examples of automotive cyber-physical attacks

Mar 2010	Command & Control Server	Over 100 cars disabled remotely by a disgruntled employee who hacked Webtech Plus, a web-based vehicle-immobilization system
May 2010	OBD II Port	Hackers killed the engine / disable the brakes of a car moving at 65 km/h using a laptop and custom software plugged into OBD II port
Jul 2014	Mobile App	Hackers remotely controlled a car's door locks, headlights, wipers, sunroof and horn while it was in motion
Jul 2015	Cellular Network	Hackers remotely control Jeep's engine while driving along a highway
Jun 2016	Wi-Fi	A Mitsubishi car's Wi-Fi was hacked allowing attackers to control its lights, unlock the doors remotely and disable the alarm
Apr 2019	Tesla Auto-pilot	Chinese hackers published a report showing how they tricked Tesla's autopilot self-driving software into swerving into oncoming traffic

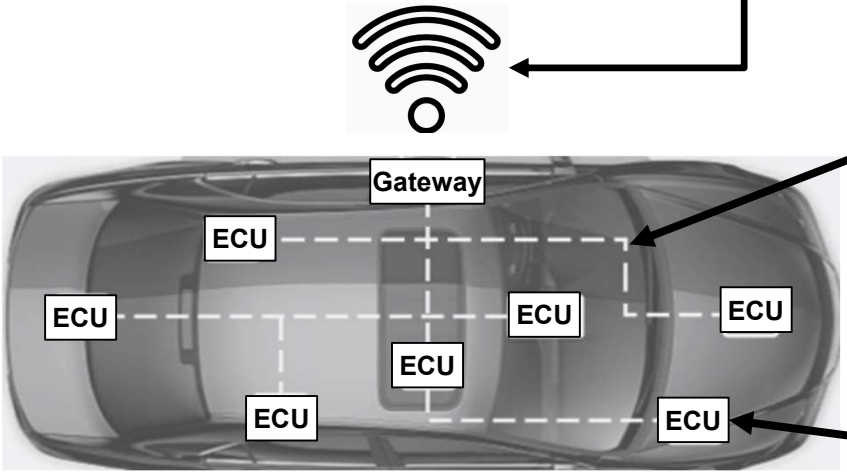
Mechanics of Cyber-Physical Attacks

Mechanics of cyber-physical attacks



Cyber-physical Attacks Target the Vehicle's Network and Embedded Software

Automotive cyber-security companies focus on protecting <u>three</u> attack vectors



Network Connectivity

1 External

BOSCH, BlackBerry, Airbiquity

2 Internal

NNG, Trillium, VECTOR

3 Embedded Software

HARMAN (A SAMSUNG COMPANY), Symantec (A Division of Broadcom), Continental

Notes: Escrypt is a subsidiary of BOSCH with focus on automotive security; Argus is subsidiary of Continental with focus on embedded software; Arilou is subsidiary of NNG with a focus on the car's internal network
Solutions may be applicable to individual cars and to fleet

Automotive Cybersecurity: Network Connectivity

Monitoring solutions require less integration at the OEM level, enabling faster sales cycles; encryption key management for IoT remains a pain point

	Monitor Monitors the flow of data over the network to detect anomalies / identify attacks	**Encryption** Secure data transfer via encryption and encryption key management
1 **External** *V2X*	Upstream.auto Securing Smart Mobility CYBER OWL	BOSCH NXP secunet utimaco® BlackBerry
2 **Internal** *CAN, FlexRay, Lin,. MOST, Ethernet*	CYMOTIVE TECHNOLOGIES SAFERIDE TECHNOLOGIES ENIGMATOS Automotive Cyber Security	VECTOR NNG Trillium

Sources: Company websites, press releases, Pitchbook, Crunchbase

Automotive Cybersecurity: Embedded Software

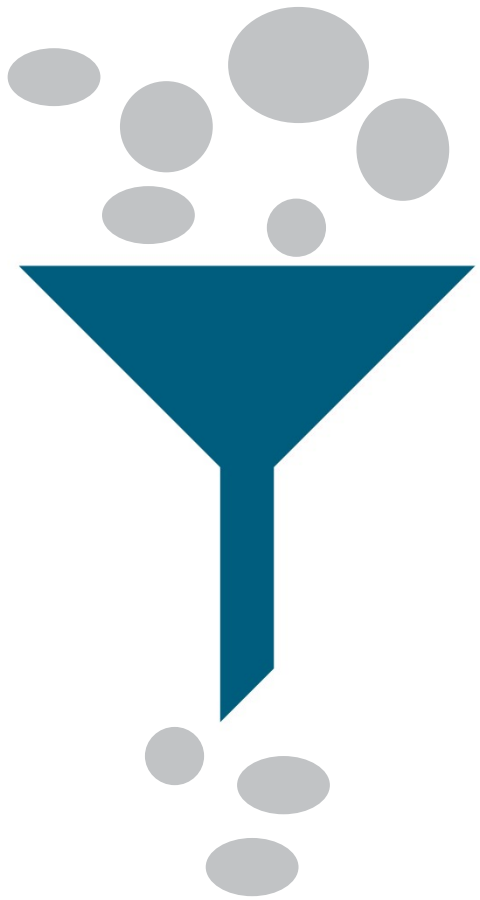
Detection & Response solutions dominated by companies w/ existing OEM relationships as they require time intensive implementation and overhead impact

	Lifecycle Protection Scan components acquired through supply chain for zero-day vulnerabilities	**Hardening** Restricts software access to firmware (e.g. MTD, Trusted Execution Environment)	**Detection & Response** Embedded agent that detects and blocks unauthorized software modification
3 **Embedded Software** *Within the ECU*	VDOO OPTIMAL+	Symantec. A Division of Broadcom MagicCube	Karamba Security HARMAN A SAMSUNG COMPANY Red Balloon Security Continental

Sources: Company websites, press releases, Pitchbook, Crunchbase

Startups Selection

How we looked at startups



KPI

Market Potential

Implications for cybersecurity for connected vehicles

- **Country Origin**: Due to access to sensitive data, US-based firms are viewed favorably
- **Product Scope**: Can the product can be applied across verticals with profitable unit economics
- **Leadership:** Strong leadership team with automotive cybersecurity experience (e.g. engineer), academic credentials (e.g. PhD), and automotive contract experience
- **Product Implementation**: Due to long sales cycle, product that are easy to deploy have a distinct advantage

Current Traction

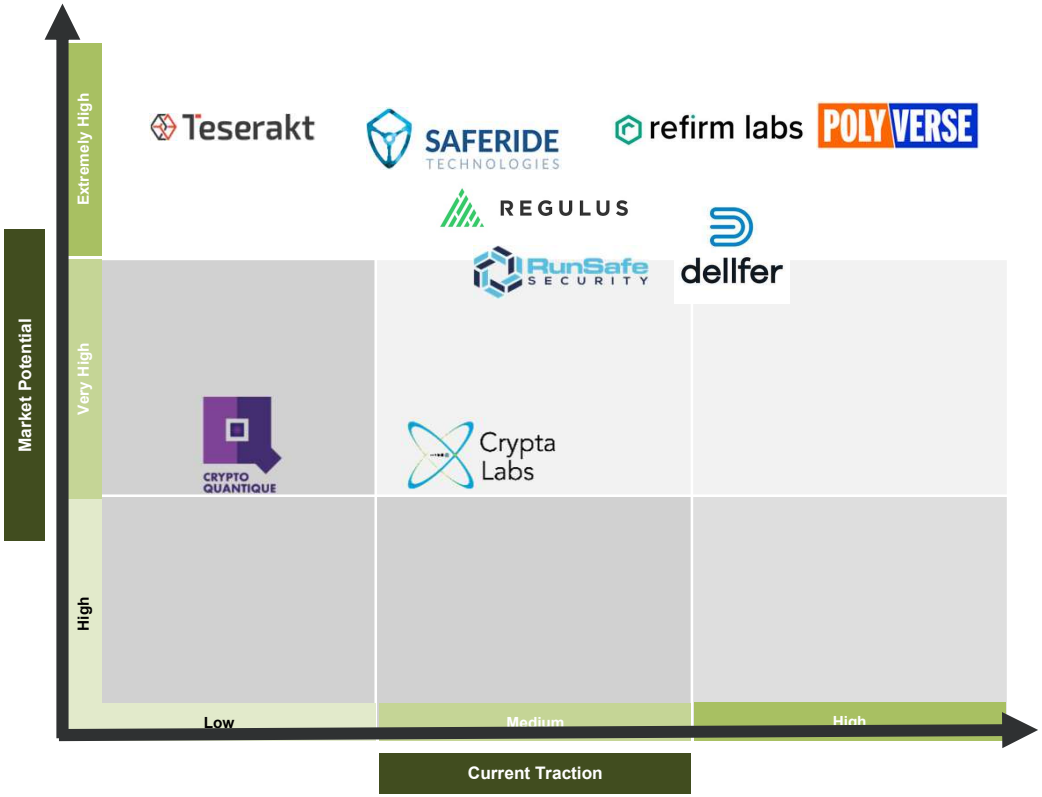
- **Revenue Stage:** Recurring revenue signals that the product is viable and in demand
- **OEM / Tier 1 Partnerships:** Established partnerships help sales and establish trustworthiness

Market map for investable areas

EVALUATION CRITERIA

MARKET POTENTIAL
- Country Origin
- Product Scope
- Leadership
- Product Implementation

CURRENT TRACTION
- Revenue Stage
- OEM / Tier 1 Partnerships



Detail – KPIs and Evaluation Criteria

	Market Potential					Traction		
	Country Origin	Product Scope	Leadership	Implementation	Total	Revenue Stage	OEM / Tier 1 Partnerships	Total
Teserakt	*2*	*3*	*3*	*3*	11	*1*	*1*	2
Regulus	*3*	*2*	*3*	*2*	10	*1*	*2*	3
SafeRide	*3*	*2*	*3*	*3*	11	*1*	*2*	3
Polyverse	*3*	*3*	*3*	*2*	11	*3*	*3*	6
ReFirm Labs	*3*	*3*	*2*	*3*	11	*3*	*2*	5
Crypta Quantique	*2*	*3*	*2*	*1*	8	*1*	*1*	3
Crypta Labs	*2*	*3*	*2*	*1*	8	*1*	*3*	4
RunSafe	*3*	*3*	*2*	*2*	10	*2*	*2*	3
Dellfer	*3*	*3*	*2*	*2*	10	*2*	*3*	5

Key

	Country Origin	Product Scope	Leadership	Implementation	Revenue Stage	Partnerships
Okay (1pt)	*Based in Country with potential US conflict (e.g. China)*	*Limited scope (e.g. only applicable to automotive industry)*	*Founders have limited experience*	*Requires integration into hardware at OEM*	*Pre-product*	*No known partnerships*
Better (2pts)	*Based in a neutral country (e.g. UK, Israel, Switzerland)*	*Potential to expand beyond the automotive industry*	*Extensive industry experience, PhD*	*Embedded software / low overhead*	*Post-product, pre-recurring revenue*	*In talks w/ partners*
Best (3pts)	*Based in the US*	*Product directly applicable to multiple industries*	*Founders / team leaders have startup experience*	*No overhead (e.g. scanning, dongle)*	*Recurring revenue*	*Established partnership w/ market leader*

1

Teserakt

Data transfer encryption for IoT devices

COMPANY

- Founded 2018 in Switzerland
- 4 Team Members
- Protects IoT data in transit via encryption

LEADERSHIP

- Jean-Philipe Aumasson, Founder, CEO, co-founder and head of security at Taurus Group, PhD in Computer Science, speaker at Black Hat, DEFCON, etc.

FUNDING

- Pre-seed, raising seed round in 2Q 2020

WHY IT IS ATTRACTIVE

- Tailored for IoT: IoT amplifies encryption key management risk; Teserakt addresses this issue via encrypting messages b/w device and message broker and via automated key rotation
- Market: Forwards and backwards compatible with all IoT devices, $0.10 / mo per device
- Product Validation: Open-source E4 software that can be vetted by experts; C2 management server is sold
- Implementation: Can easily be implemented into IoT environments via software library or a source code component; minimal overhead impact

POTENTIAL RISKS

- Sales cycle: despite ease of integration, slow sales cycle for B2B security may delay adoption
- Traction: there is proof of concept and there have been some sales, but Teseakt is pre-recurring revenue
- Endpoint security: Teserakt secures data transfer between endpoints, but does not secure the endpoints themselves

Network - External: Regulus Cyber

2

REGULUS

Defense against GNSS spoofing and GPS hacking for cars

COMPANY

- Founded 2016 in Haifa, Israel
- 15 Team Members
- Detects and protects against GNSS spoofing

LEADERSHIP

- Yonatan Zur and Yoav Zangvil, Co-founders & CEO/CTO, extensive expertise in relevant fields with the Israeli army and defense industries

FUNDING

- $6.3M raised (series A - Sierra Ventures, Canaan Partners, F2 Capital)
- $3.5M committed from current and new investors
- Looking for +$0.5M in April 2020 (gap financing)

WHY IT IS ATTRACTIVE

- Product validation: already performed tests with multiple OEMs, and in various industries dependent on GNSS.
- Market: Large market size of connected cars, mobile devices, IoT, plus strong interest from telco and ride-hailing. 7% of world's GDP depends directly on GNSS functioning.
- Ease of implementation: affordable; stand-alone; hardware-agnostic and OTA-update-enabled. First stand alone "anti virus" software for GNSS
- Strong expertise: team of expert GNSS and multidisciplinary engineers from Israeli defense forces and various industry leading companies.

POTENTIAL RISKS

- Traction: Regulus Cyber is pre-recurring revenue, however, major deals are expected to close in Q1-Q2 2020. Various POCs, some paid, with automotive, mobile, and IoT corporations are in place

Network - Internal: SafeRide Technologies

3

SAFERIDE TECHNOLOGIES

AI based anomaly detection for connected cars

COMPANY

- Founded 2016 in Tel Aviv, Israel
- 35 Team Members
- AI-based vehicle health monitoring software detecting malfunctions and zero-day cyber threats

LEADERSHIP

- Yossi Vardi, co-founder and CEO, co-founded/led/ funded / helped build > 80 high-tech companies
- Hilik Stein, co-founder & CTO, 25+ years in tech/cybersecurity (ex. Cisco, Radware)

FUNDING

- $10M Seed + series A -
  ST Engineering / TEMASEK
  Irdeto / NASPERS
- Interest in series B

WHY IT IS ATTRACTIVE

- Product validation: 3 major evaluations finished in 2019 – 1 in US, 2 in Europe; All three resulted in pilot projects in 2020
- Market: Large market size of connected cars cybersecurity solutions, and applications for automotive OEM cost reduction (vehicle health monitoring improves fleet uptime; data compression reduces cost to upload on cloud)
- Strong R&D expertise: data scientists (incl. 3 PhDs), Cybersecurity researchers (ex-military, ex-NSO), embedded software experts, and network communication experts

POTENTIAL RISKS

- Traction: no long-term clients yet, but successful large customer evaluations in 2019 that led to pilots starting 1Q 2020

Embedded Software: Polyverse

4

POLYVERSE

Provider of Linux hardened operating systems to stop memory-based attacks

COMPANY

- Founded in 2015 (Bellevue, WA)
- Employees: 20
- Stage: Early Series A

LEADERSHIP

- **Alex Gounares:** Co-Founder/CEO, BS Computer Science (Princeton), Former AOL CTO, Founder of Concurix, Former CTO Of Microsoft's Online Services Division
- **Archis Gore:** Co-Founder/CTO, MS Computer Science, software engineer at Amazon and Microsoft

FUNDING

Date	Stage	Raised	Post Val	Lead Investors
Jul-15	Seed	$1M	$5M	Clear Fir Partners
May-17	Seed	$4M	$30M	SpringRock Ventures
Jan-20	Series A	$8M		

WHY IT IS ATTRACTIVE

- Generating revenue and profitable
  - Licensing model for recurring revenue
- Contracts with U.S. Government for use on drones
  - Sole Source J&A
- Demonstrated proof of concept
- In early stage talks with two auto manufacturers
- Targets the largest source of cybersecurity attacks

POTENTIAL RISKS

- Currently small team
  - Using money to build sales force
- Product – Market Fit in vehicle industry
  - Reactionary environment and complacency among customer base
- Education process

Embedded Software: ReFirm Labs

5

refirm labs

US-based Cybersecurity platform for Embedded Systems

COMPANY

- Scans firmware for existing vulnerabilities to prevent zero-day attacks
- Team expertise in national defense cybersecurity
- US-based Team

LEADERSHIP

Derick Naef, CEO & Co-Founder

- Former NSA security analyst
- Successful Exit

Terry Dunlap, Co-Founder

- Former Deloitte Cybersecurity
- Former NSA security analyst
- Successful Exit

Funding

- 3.5M in funding, Data Tribe

WHY IT IS ATTRACTIVE

- Annual Subscription-based revenue model that fits into development cycle
- Large market potential – firmware protection becoming increasingly important in IoT
- Applicable for both existing and future connected devices
- Non-intrusive, automated solution promotes a faster sales cycle
- US-based, increasing trust and expanding potential customer base
- Established implementation partnership with Deloitte Cyber

POTENTIAL RISKS

- Building trust to upload firmware image without human component
- Well established competitors in the connected car space (Karamba, VDOO)
- Limited in scope to Firmware-based vulnerabilities

Other startups considered (1 of 3): Network - External

Company (stage, launch)	Total raised	Notable investors	Description	Pros/Cons
CRYPTO QUANTIQUE (Seed, 2016)	$17.4M	Accelerated Digital Ventures; Entrepreneur First	End-to-end encryption key management platform using device-based key generation, removing key injection and key-transfer	✓ Removes pain-point of trusting the transfer of encryption keys via device-based key generation × Hardware-based solution w/ cloud service complicates the sales process; pre-revenue w/ proof of concept expected 2Q 2020
Crypta Labs (Seed, 2015)	$3.7M	Bloc Ventures	Quantum random number generation for the Cooperative Intelligent Transport Systems for Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication	✓ Future-proof QRNG; awarded £1.2M UK govt. funding from Future of Mobility Grand Challenge for automotive cybersecurity in Jan 2020 × Hardware-based solution; only applicable for large IoT devices (e.g. cars) due to size limitations; miniaturization required for broader adoption
TESKALABS (Seed, 2014)	$0.6M	StartupYard	Developer of cloud-based security products designed to provide Mobile and IoT application security	✓ PKI product used in consortium w/ Crypta Labs and IDIADA; awarded £1.2M UK govt. funding from Future of Mobility Grand Challenge for automotive cybersecurity in Jan 2020 × Provides public key infrastructure only; must be used in concert with encryption provider

Sources: Company websites, press releases, Pitchbook, Crunchbase, interviews

Other startups considered (2 of 3): Network - Internal

Company (stage, launch)	Total raised	Notable investors	Description	Pros/Cons
C2A security (Series A, 2016)	$7.7	Israel Cleantech Ventures	End-to-end cybersecurity platform that detects and mitigates attacks	✓ End-to-end platform involved from planning to OEM production to active management of × Multilayered solution may result in a longer sales cycle
CYBER OWL (Seed, 2016)	$3.4M	Mercia Asset Management;	Cyber-physical risk analytics platform that provides real-time visibility into vehicle fleet security	✓ Threat-level security risk monitoring platform can be applied to variety of verticals (currently defense, utilities, maritime, etc.); raised £1M in June 2019 × Product provides threat intelligence but doesn't actively provide attack response; applicable but not currently focused on automotive industry
CYMOTIVE TECHNOLOGIES (Corporate Backed, 2016)	Un-known	Volkswagen	Prevents data sniffing via OBD II dongle product, monitors internal network w/ IDS, and provides real-time visibility on fleet health	✓ Working directly with Volkswagen reduces the sales risk of having to sell this product to an automotive company × Ownership structure: Volkswagen holds 40% of shares
ENIGMATOS Automotive Cyber Security (Angel / pre-seed, 2015)	$0 (undisclosed angel investments)	NA	Provides deep car identity profiling and analysis of messages on the network to detect anomalies and recommend counter-actions	✓ Post-revenue (although early stage): partnerships with commercial vehicle fleets in Israel (Pelephone cars and Orpak), discussions with OEMs and other potential customers × Only present in Israel

Sources: Company websites, press releases, Pitchbook, Crunchbase, interviews

Other startups considered (3 of 3): Embedded Software

Company (stage, launch)	Total raised	Notable investors	Description	Pros/Cons
MagicCube (Series A, 2014)	$9.9M	EPIC Ventures, Azure Capital Partners, Silicon Valley Bank	Provides software-based Trusted Execution Environment (TEE) for device protection	✓ Software-based solution that provides security around ECUs that usually require a hardware solution × Inability to integrate into existing devices
RunSafe Security (Series A, 2015)	$8.9M	Alsop Louie Partners; Working Lab Capital	Hardens embedded software by changing the attack surface; creates unique memory layout so exploits can't find function or sequence it's looking to exploit	✓ Implements in hours w/ <1% overhead impact (vs. Karamba that takes months to implement and has 5-10% overhead impact) × Does not currently provide monitoring software that would alert customers of an attempted / successful breach
RazorSecure (Series A, 2014)	$5.3M	Breed Reply; Mainport Innovation Fund II	Uses artificial intelligence to identify how a system normally operates, and identifies deviation as a possible threat	✓ Operates without connection to the internet × Potential issues with false positives given the use of machine learning to detect anomalies
dellfer (Seed, 2016)	$2.5M	Denso International; Sand Hill Angels	Protects embedded systems against unknown zero-day attacks using a runtime integrity protection platform	✓ Partnership with Denso will expand sales reach and accelerate adoption × Remediation of an attack once detected is unclear

Sources: Company websites, press releases, Pitchbook, Crunchbase, interviews

APPENDIX

Startups and Experts Consulted

STARTUP OPERATORS

- Polyverse, CEO
- ReFirm Labs, CEO
- Arbiquity, (VP of Marketing)
- VDOO, VP of Marketing
- Crypta Labs, CCO
- Teserakt, CEO
- Savari, PM
- Altr
- Dispel, CEO
- Regulus Cyber (CBIO)
- SafeRide Tech (VP Product Mgmt)
- Runsafe, CEO
- Crypto Quantique, CEO
- Cymotive, Co-Founder

SMEs

- Chris Valasek, Autonomous Vehicle Security Architect at Cruise
- Federicco Maggi, Sr. Researcher at Trend Micro
- Sean Batir, Sr. ML Engineer at BMW
- Scott Frank, VP Marketing at Airbiquity
- Others not included due to NDA

Selected Automotive Cybersecurity Companies

Company	Founded	Total Fundraised ($M)	Stage	External Data Management	Internal Network	Embedded Software
Harman (Samsung)	1980	--	Mature			x
NXP	1953	--	Mature	x	x	
ETAS (Bosch)	1994	--	Mature	x		
Vector Informatik (MTM)	1988	--	Mature	x	x	
Symantec (Broadcom)	1982	--	Mature			x
Arilou (NNG)	2004	--	Mature		x	
secunet	1997	--	Mature	x		
Utimaco (EQT)	1983	--	Mature	x		
Aptiv	2008	--	Mature	x		
Denso	1949	--	Mature	x		
Continental	1870	--	Mature			x
Onboard Security (QualComm)	2017	--	Mature	x		
Blackberry	1999	--	Mature	x	x	x
Airbiquity	1997	--	Later Stage VC	x		
Otonomo Technologies	2015	$53	Later Stage VC	x		
Optimal+	2005	$72	Later Stage VC			x
Centri	2009	$27	Later Stage VC	x		
Upstream	2017	$41	Later Stage VC		x	
VDOO	2017	$45	Later Stage VC			x
Karamba	2015	$27	Later Stage VC			x

Sources: Company websites, press releases, Pitchbook, Crunchbase

Selected Automotive Cybersecurity Companies

Company	Founded	Total Fundraised ($M)	Stage	External Data Management	Internal Network	Embedded Software
GuardKnox	2016	$24	Series A		x	
Red Balloon Security	2011	$22	Series A			x
Polyverse	2015	$17	Series A			x
Trillium Secure	2014	$15	Series A		x	
MagicCube	2014	$11	Series A			x
RunSafe Security	2015	$9	Series A			x
Regulus Cyber	2016	$8	Series A	x		
C2A Security	2016	$7	Series A		x	x
Razor Secure	2014	$5	Series A			x
Crypto Quantique	2016	$17	Seed	x		
SafeRide	2018	$8	Seed		x	
Refirm Labs	2017	$4	Seed			x
Crypta Labs	2014	$4	Seed	x		
Dellfer	2016	$2	Seed			x
ALTR	2014	$15	Angel	x		
Teserakt	2018	<$1	Pre-Seed	x		
CyberOwl	2016	$1	Pre-Seed		x	
TeskaLabs	2014	$1	Pre-Seed	x		
Cymotive Technologies	2016	N/A	Joint Venture		x	
Enigmatos	2015	Undisclosed	Undisclosed		x	

Sources: Company websites, press releases, Pitchbook, Crunchbase